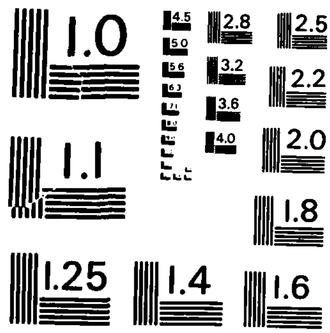
AD-A163 626 THE CHINESE REMAINDER PROBLEM AND POLYNOMIAL INTERPOLATION(U) WISCONSIN UNIV-MADISON MATHEMATICS RESEARCH CENTER I J SCHOENBERG NOV 85 MRC-TSR-2889 1/1

UNCLASSIFIED DAAG29-80-C-0041 F/G 12/1 NL



MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

AD-A163 626

MRC Technical Summary Report #2889

THE CHINESE REMAINDER PROBLEM AND POLYNOMIAL INTERPOLATION

I. J. Schoenberg

Mathematics Research Center
University of Wisconsin—Madison
610 Walnut Street
Madison, Wisconsin 53705

November 1985

(Received November 5, 1985)

Approved for public release
Distribution unlimited

Sponsored by

U. S. Army Research Office
P. O. Box 12211
Research Triangle Park
North Carolina 27709

UNIVERSITY OF WISCONSIN - MADISON
MATHEMATICS RESEARCH CENTER

THE CHINESE REMAINDER PROBLEM AND POLYNOMIAL INTERPOLATION

I. J. Schoenberg

Technical Summary Report #2889

November 1985

ABSTRACT

Let

$$m_i (i=1,\dots,n) \tag{1}$$

be positive integers pairwise relatively prime. The Chinese Remainder Problem is to find a solution x of the n congruences

$$x \equiv a_i (\mathrm{mod}\ m_i) \quad (i=1,\dots,n) \quad . \tag{2}$$

where the integers a_i are given. From Marcel Riesz I learnt orally that this problem is an analogue of the problem of finding a polynomial $P(x)$ of degree $n-1$ which solves the interpolation problem

$$P(x_i) = y_i (i=1,\dots,n) \ (y_i \text{ given and also distinct } x_i) \quad . \tag{3}$$

This is solved by Lagrange's interpolation formula

$$P(x) = \sum_{i=1}^{n} y_i L_i(x) \tag{4}$$

where $L_i(x)$ are the fundamental functions satisfying

$$L_i(x_j) = \delta_{ij} \quad . \tag{5}$$

Also (2) can be similarly solved by determining the $b_i (i=1,\dots,n)$ satisfying the congruences

$$b_i \equiv \delta_{ij} (\mathrm{mod}\ m_j) \tag{6}$$

Theorem 1. *A solution of the system (2) is given by*

$$x = \sum_{i=1}^{n} a_i b_i \quad . \tag{7}$$

Besides recording this analogy of Marcel Riesz, the author's contribution is the following remark: Just as Newton solves the problem (3) successively with his formula using successive divided differences, it is convenient to solve the system (2) successively obtaining

Theorem 2. *The integer*

$$x = a_1 + d_1 m_1 + d_2 m_1 m_2 + \dots + d_{n-1} m_1 m_2 \cdots m_{n-1} \tag{8}$$

is a solution of (2) if we determine the $d_i (i=1,\dots,n-1)$ *successively by the congruences*

Sponsored by the United States Army under Contract No. DAAG29-80-C-0041.

$$
(9)\qquad
\begin{aligned}
& a_1 + d_1 m_1 \equiv a_2 \pmod{m_2} \\
& a_1 + d_1 m_1 + d_2 m_1 m_2 \equiv a_3 \pmod{m_3} \\
& \quad \vdots \\
& a_1 + d_1 m_1 + \cdots + d_{n-1} m_1 \cdots m_{n-1} \equiv a_n \pmod{m_n} \;.
\end{aligned}
$$

Indeed, from (9) we find that

$$x = a_1 + d_1 m_1 + \cdots + d_{k-1} m_1 m_2 \cdots m_{k-1} \equiv a_k \pmod{m_k}$$

for $k = 1,\ldots,n$.

AMS (MOS) Subject Classifications: 10A10, 41A05

Key Words: Chinese Remainder Problem, Polynomial Interpolation

Work Unit Number 6 - Miscellaneous Topics

SIGNIFICANCE AND EXPLANATION

The Chinese Remainder Problem (Ch.R.P) is to find an integer x such that

$$x \equiv a_i (\text{mod } m_i) \quad (i=1,\ldots,n) \quad ,$$

where m_i are pairwise relatively prime moduli and a_i are given integers. In the 1950's I learnt orally from Marcel Riesz that the CH.R.P. is an analogue of the polynomial interpolation problem

$$P(x_i) = y_i (i=1,\ldots,n) \quad , \quad P(x) \in \pi_{n-1} \quad ,$$

and that the Ch.R.P. can be solved by an analogue of Lagrange's interpolation formula. The author now adds the remark that the Ch.R.P. can be solved, even more economically, by an analogue of Newton formula using successive divided differences.

The responsibility for the wording and views expressed in this descriptive summary lies with MRC, and not with the author of this report.

THE CHINESE REMAINDER PROBLEM AND POLYNOMIAL INTERPOLATION

I. J. Schoenberg

Let

(1) $m_i (i=1,\ldots,n)$ be positive integer s.t. $(m_i, m_j) = 1$ if $i \neq j$.

The Chinese remainder problem is as follows

<u>The Problem</u>. <u>Given the integers</u> $a_i (i=1,\ldots,n)$ <u>we are to find an interger</u> x <u>satisfying the congruences</u>

(2) $$x \equiv a_i (\text{mod } m_i) \quad , \quad (i=1,\ldots,n) \quad .$$

Sometime in the nineteen-fifties Marcel Riesz visited the Universit; c Pennsylvania and told us informally that the problem (2) can be thought o1 is an analogue of the problem of finding a polynomial $P(x)$ of degree $n-1$ solving the interpolation problem

(3) $$P(x_i) = y_i (i=1,\ldots,n), \quad (y_i \text{ given and also distinct } x_i) \quad .$$

This problem is solved by Lagrange's formula

(4) $$P(x) = \sum_1^n y_i L_i(x) \quad ,$$

where the fundamental functions $L_i(x)$ are defined by

(5) $$L_i(x_j) = \delta_{ij}, \quad (i,j=1,\ldots,n) \quad .$$

Similarly, if we define the integers b_i by the congruences

(6) $$b_i \equiv \delta_{ij} (\text{mod } m_j) \quad (i,j=1,\ldots,n) \quad ,$$

we have

<u>Theorem</u> 1. <u>A solution of the system (2) is given by</u>

(7) $$x = \sum_1^n a_i b_i \quad .$$

Indeed, as soon as we have the b_i satisfying (6), we easily see that the integer x satisfies (2). Clearly the integers a_i are the analogues of

---

Sponsored by the United States Army under Contract No. DAAG29-80-C-0041.

the y_i of (3), while the integers b_i of (6) are the analogues of the fundamental functions $L_i(x)$ of (5).

Our solution of (2) by means of (6) is essentially also the solution as given in [1, 66-71] and [2, 49-51] without mentioning the analogy with Lagrange's formula (4).

Besides recording Riesz's remark, the author's contribution is the following remark: Newton solves the interpolation prolem (3) successively using successive divided differences. Applying Newton's idea to the solution of the congruences (2) we obtain the following procedure:

Determine the integers

$$d_i (i = 1,2,\dots,n-1) \tag{8}$$

so as to satisfy the $n-1$ congruences

$$\begin{aligned} & a_1 + d_1m_1 \equiv a_2 \pmod{m_2} \\ & a_1 + d_1m_1 + d_2m_1m_2 \equiv a_3 \pmod{m_3} \\ & \quad \vdots \\ & a_1 + d_1m_1 + d_2m_1m_2+\dots+d_{n-1}m_1m_2\cdots m_{n-1} \equiv a_n \pmod{m_n} \ . \end{aligned} \tag{9}$$

Notice he triangular shape of this system: We determine first a value of m_1, then m_2 a.s.f. The d_i having been determined we have

Theorem 2. A solution of the system (2) is given by

$$x = a_1 + d_1m_1 + d_2m_1m_2+\dots+d_{n-1}m_1m_2\cdots m_{n-1} \ . \tag{10}$$

Indeed, from (9) we find that

$$x \equiv a_1 + d_1m_1+\dots+d_{k-1}m_1m_2\cdots m_{k-1} \equiv a_k \pmod{m_k}$$

for $k = 1,2,\dots,n$, because of the $(k-1)$st congruence (9).

Remarks. 1. The seond Newton approach is slightly more economical: While the Lagrange approach required to find the n integers b_i, the Newton approach required to determine only $n-1$ integers $d_i (i=1,2,\dots,n-1)$.

2. The analogy with Newton's solution of (3): The d_i of (10) correspond to the successive divided differences, and the m_i are the analogues of the $x-x_i$.

REFERENCES

1. G. E. Andrews, Number Theory, W. B. Saunders Co., Philadelphia, 1971.
2. Emil Grosswald, Topics from the Theory of Numbers, The Macmillan Co., New York, 1966.

IJS/jvs

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER #2889	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) The Chinese Remainder Problem and Polynomial Interpolation		5. TYPE OF REPORT & PERIOD COVERED Summary Report - no specific reporting period
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) I. J. Schoenberg		8. CONTRACT OR GRANT NUMBER(s) DAAG29-80-C-0041
9. PERFORMING ORGANIZATION NAME AND ADDRESS Mathematics Research Center, University of Wisconsin 610 Walnut Street Madison, Wisconsin 53706		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS Work Unit Number 6 - Miscellaneous Topics
11. CONTROLLING OFFICE NAME AND ADDRESS U. S. Army Research Office P.O. Box 12211 Research Triangle Park, North Carolina 27709		12. REPORT DATE November 1985
		13. NUMBER OF PAGES 4
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)		15. SECURITY CLASS. (of this report) UNCLASSIFIED
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Chinese Remainder Problem, Polynomial Interpolation

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

Let

(1) $$m_i \ (i=1,\dots,n)$$

be positive integers pairwise relatively prime. The Chinese Remainder Problem is to find a solution x of the n congruences

(2) $$x \equiv a_i (\mathrm{mod}\ m_i) \ (i=1,\dots,n) \ .$$

where the integers a_i are given. From Marcel Riesz I learnt orally that this problem is an analogue of the problem of finding a polynomial $P(x)$ of

ABSTRACT (continued)

degree $n-1$ which solves the interpolation problem

(3) $P(x_i) = y_i (i=1,\dots,n)$ (y_i given and also distinct x_i) .

This is solved by Lagrange's interpolation formula

(4) $$P(x) = \sum_{i=1}^{n} y_i L_i(x)$$

where $L_i(x)$ are the fundamental functions satisfying

(5) $$L_i(x_j) = \delta_{ij} \quad .$$

Also (2) can be similarly solved by determining the $b_i(i=1,\dots,n)$ satisfying the congruences

(6) $$b_i \equiv \delta_{ij} (\bmod\ m_j)$$

Theorem 1. A solution of the system (2) is given by

(7) $$x = \sum_{i=1}^{n} a_i b_i \quad .$$

Besides recording this analogy of Marcel Riesz, the author's contribution is the following remark: Just as Newton solves the problem (3) successively with his formula using successive divided differences, it is convenient to solve the system (2) successively obtaining

Theorem 2. The integer

(8) $$x = a_1 + d_1 m_1 + d_2 m_1 m_2 + \dots + d_{n-1} m_1 m_2 \cdots m_{n-1}$$

is a solution of (2) if we determine the $d_i(i=1,\dots,n-1)$ successively by the congruences

(9) $$\begin{aligned} &a_1 + d_1 m_1 \equiv a_2 (\bmod\ m_2) \\ &a_1 + d_1 m_1 + d_2 m_1 m_2 \equiv a_3 (\bmod\ m_3) \\ &\quad\vdots \\ &a_1 + d_1 m_1 + \dots + d_{n-1} m_1 \cdots m_{n-1} \equiv a_n (\bmod\ m_n) \quad . \end{aligned}$$

Indeed, from (9) we find that

$$x = a_1 + d_1 m_1 + \dots + d_{k-1} m_1 m_2 \cdots m_{k-1} \equiv a_k \ (\bmod\ m_k)$$

for $k = 1,\dots,n$.

END
FILMED
3-86
DTIC